DESCRIPTION

ENCRYPTION DEVICE AND ENCRYPTION METHOD

Technical Field

This invention relates to an encryption device and an encryption method and, more particularly, applied to a case of encrypting information (hereinafter, referred to as identification information) that is used to prove validly of an identification target.

Background Art

Heretofore, an encryption device adopting a secret key encryption method or a public key encryption method is designed to create encrypted identification information by performing prescribed encryption on identification by using encryption key information being stored in an internal non-volatile memory and send this to a decryption device.

In this case, the encryption device ensures reliability of an encryption function by preventing encryption key information being stored in the non-volatile memory from being stolen. As a method of preventing the encryption key information from being stolen, a non-volatile memory is installed between units at a deep part of the encryption device, or a non-volatile memory and an encryption/decryption unit for encrypting encryption key

information only when the information is stored in the non-volatile memory are installed as one tip (for example, refer to Patent Reference 1).

Patent Reference 1 Japanese Patent Laid-open No. 2003-256282

However, such an encryption device is not enough to offer reliability of an encryption function because not only installation of a non-volatile memory is complicated but also encryption key information cannot be prevented from being stolen from the non-volatile memory.

This invention has been made in view of foregoing and proposes an encryption device and encryption method capable of improving reliability of an encryption function.

To solve the above problem, this invention provides an encryption device for encrypting information on a confidential target with: a creation means for creating a unique parameter of an element group, based on a signal output from the element group internally having a plurality of elements as a unit; and an encryption means for encrypting information by using the unique parameter created by the creation means.

Further, this invention provides an encryption method of encrypting information on a confidential target with: a first step of creating a unique parameter of an element group, based on a signal output from the element group internally having a

plurality of elements as a unit; and a second step of encrypting information by using the created unique parameter.

As described above, according to this invention, information is encrypted by using a unique parameter of an internal element group. This means that encryption can be performed by using a unique parameter that third parties cannot detect, even in manufacturing, without previously storing the parameter in a non-volatile memory or the like, thereby being capable of easily ensuring confidentiality of identification information D1 and thus improving reliability of an encryption function.

Brief Description of the Drawings

Fig. 1 is a block diagram showing a construction of an identification system.

Fig. 2 is a block diagram showing a construction of an encryption device according to this embodiment.

Fig. 3 is a schematic diagram showing a construction of an imaging unit.

Fig. 4 is a block diagram showing a construction of a decryption device.

Best Mode for Carrying out the Invention

One embodiment of this invention will be described in detail with reference to the accompanying drawings.

(1) Construction of identification system

Referring to Fig. 1, reference numeral 1 shows an identification system according to this embodiment, in which a plurality of encryption devices 2 (2A to 2N) serving as communication sources are wirelessly connected to a decryption device 3 serving as a communication party so that the encryption devices 2 and the decryption device 3 can communicate_various kinds of information with each other.

In this case, an encryption device 2 creates a characteristic pattern of a prescribed part of a user using this encryption device 2 as identification information when starting communication with the decryption device 3. Then the encryption device 2 creates encrypted identification information by encrypting this identification information and sends this to the decryption device 3.

The decryption device 3, on the other hand, restores the identification information by decrypting the received encrypted identification information, and compares this identification information with corresponding registered information previously registered.

The decryption device 3 continues the communication of information with the encryption device 2 only when it is determined based on the comparison result that the user using the encryption device 2 sending the identification information is a rightful registrant.

As described above, in this identification system 1,

validity of a user using the encryption device 2 is determined by using body information on the user.

(2) Construction of encryption device

Since the encryption devices 2 (2A to 2N) are identical, the construction of the encryption device 2A will be now described.

Referring to Fig. 2, the encryption device 2A is composed of an imaging unit 11 for imaging blood vessels inside a finger as an imaging target, an identification information creation unit 12 for creating identification information based on the imaging result of the imaging unit 11, an encryption unit 13 for encrypting the identification information, and a communication unit 14 for communicating information through a communication process with a prescribed radio communication scheme.

This imaging unit 11 is designed to image blood vessels by using such a feature that light (near-infrared light) of near-infrared light bandwidth is specifically absorbed in deoxygenization hemoglobin (venous blood) or oxygenation hemoglobin (arterial blood) in the blood vessels.

In actual, as shown in Fig. 3, the imaging unit 11 has one or two or more light sources 21 for emitting near-infrared light (three light sources are shown in Fig. 3). On the light path of the near-infrared light which is emitted from the light sources 21, a first filter 22 for allowing specific light of near-infrared light bandwidth out of the near-infrared light to pass therethrough, a second filter 23 for allowing light of near-

infrared light bandwidth which is absorbed in venous bloods and its adjacent light out of light obtained via the first filter 22 to pass therethrough, and a solid imaging element 24 are provided in order.

In addition, the imaging unit 11 is provided with a diffusion plate 26_at a position (hereinafter, referred to as out-of-light-path position) P1 other than on the light path of the near-infrared light. This diffusion plate 26 can move between the out-of-light-path position P1 and a position (hereinafter, referred to as on-light-path position) P2 a prescribed distance away from the solid imaging element 24.

Furthermore, in this imaging unit 11, a finger FG can be inserted between the first filter 22 and the second filter 23, and a shielding unit 25 for blocking the outside light in the air out of the light path of the near-infrared light while the finger FG is inserted is provided, thereby being capable of reducing influences of visible light and ultraviolet radiation existing out of the shielding unit 25 on the near-infrared light in imaging the blood vessels inside the finger FG.

In this case, when the imaging unit 11 receives an imaging command while the finger FG is inserted between the first and second filters 22 and 23, it emits near-infrared light from the light sources 21 and irradiates the finger FG with the light via the first filter 22.

Since this near-infrared light is specifically absorbed in

intrinsic hemoglobin in the blood vessel tissues inside the finger FG, the near-infrared light obtained through the finger FG enters the solid imaging element 24 via the second filter 23 as a blood vessel pattern light representing a formation pattern of the blood vessel tissues.

Then the imaging unit 11 performs photoelectric conversion on the blood vessel pattern light with a plurality of photoelectric conversion elements arranged in the solid imaging element 24, and sends a blood vessel image signal S1 created by the photoelectric conversion elements to the identification information creation unit 12 (Fig. 2).

In this way, the imaging unit 11 can image blood vessels inside a body as an imaging target.

The identification information creation unit 12 creates blood vessel image data by performing A/D (Analog/Digital) conversion on the received blood vessel image signal S1, and extracts blood vessels of a previously specified region from the blood vessel image based on the blood vessel image data. Then the identification information creation unit 12 creates a formation pattern of the extracted blood vessels as identification information D1 and sends this to the encryption unit 13.

The encryption unit 13 has a memory (hereinafter, referred to as encryption key information memory) 13a for storing a plurality of encryption key information sequentially created with a prescribed algorithm, and selects and reads, for example,

encryption key information D21 corresponding to a request made from the decryption device 3 (Fig. 1) via the communication unit 14, from the plurality of encryption key information D2 ($D2_1$ to $D2_n$) being stored in the encryption key information memory 13a.

Then the encryption unit 13 creates encrypted identification information D3 by encrypting the received identification information D1 by using the read encryption key information $D2_1$ with, for example, the AES (Advanced Encryption Standard), and sends this to the decryption device 3 (Fig. 1) via the communication unit 14.

Since the encryption device 2A creates the identification information D1 representing a blood vessel formation pattern unique to an inside of the body in this way, direct stealing from a body can be prevented as compared with a case of creating fingerprints existing on a surface of a body as identification information, thus being capable of previously preventing a user using the encryption device 2A from pretending he/she is a registrant.

(3) Encryption key information creation process

In addition to the above configuration, this encryption device 2A is designed to create a plurality of encryption key information D2 ($D2_1$ to $D2_n$) unique to this encryption device 2A based on a result of imaging a uniform imaging target with the imaging unit 11.

In this case, the encryption device 2A is designed to

perform a prescribed encryption key information creation process every time when receiving a creation request of encryption key information via the communication unit 14 from the decryption device 3 (Fig. 1), and store or update the created encryption key information D2 in the encryption key information memory 13a of the encryption unit 13. An encryption key information creation unit 15 for performing this encryption key information creation process will be now described.

When the decryption device 3 makes a creation request, the encryption key information creation unit 15 makes the imaging unit 11 image a uniform imaging target, and creates encryption key information based on a signal which is obtained as the imaging result.

In actual, the encryption key information creation unit 15 controls the diffusion plate 25 of the imaging unit 11 (Fig. 3) so as to move from the out-of-light-path position P1 to the on-light-path position P2, and sends an imaging command to the imaging unit 11.

In this case, in the imaging unit 11 (Fig. 3), the diffusion plate 25 is irradiated with near-infrared light emitted from the light sources 21 via the first and second filters 22 and 23 in order, and diffuses the light toward the solid imaging element 24 as uniform diffused light (hereinafter, referred to as uniform diffused light), so that the light enters the solid imaging element 24.

This solid imaging element 24 is provided with openings and light collective lens corresponding to a plurality of photoelectric conversion elements arranged in a matrix in the solid imaging element 24. These openings and light collective lens have different sizes due to various causes in manufacturing and this variation is unique to the solid imaging element 24.

Therefore, a signal (hereinafter, referred to as uniform image signal) S2 input to the encryption key information creation unit 15 (Fig. 2) as a result of performing the photoelectric conversion on the uniform diffused light at the solid imaging element 24 includes the variation unique to the solid imaging element 24, which cannot be known in manufacturing, as a noise pattern (hereinafter, referred to as variation pattern).

The encryption key information creation unit 15 creates uniform image data by performing the A/D conversion on the uniform image signal S2 obtained as described above, and creates a parameter (hereinafter, referred to as element-specific parameter) attribute to the unique variation pattern of the solid imaging element 24 based on the unique image data.

In this embodiment, as a method of creating the element-specific parameter, the encryption key information creation unit 15 calculates a hamming distance of a uniform image data and a prescribed evaluation pattern data and creates an element-specific parameter from the calculation result.

Specifically, the encryption key information creation unit

15 has an information memory 15a storing, for example, three data strings which are different in hamming_distance, as evaluation patterns A_{EV}, B_{EV}, and C_{EV}. By using these evaluation patterns A_{EV}, B_{EV}, and C_{EV}, taking as "X" higher-ranked uniform image data (hereinafter, referred to as higher-ranked uniform image data) of the same data length as the evaluation patterns out of the uniform image data, and taking an eXclusive OR (XOR) as "^", and with the following equation,

$$dH(x, A_{EV}) = \Sigma xi \hat{} Ai = Xa$$
$$dH(x, B_{EV}) = \Sigma xi \hat{} Bi = Xb \quad \text{.....(1)}$$
$$dH(x, C_{EV}) = \Sigma xi \hat{} Ci = Xc$$
$$\text{where } i = 1 \text{ to } n$$

the encryption key information creation unit 15 calculates the hamming distance Xa, Xb, Xc of the higher-ranked uniform image data Z and each of the evaluation patterns A_{EV}, B_{EV}, and C_{EV}, and combines the hamming distances Xa, Xb and Xc, thereby creating an element-specific parameter.

In this case, the encryption key information creation unit 15 can keep repeatability of the element-specific parameter obtained due to a variation pattern even in a case where uniform image data varies according to the imaging situations at the time of imaging. This is because the element-specific parameter is created from correlation results between the higher-ranked uniform

image data X and the evaluation patterns A_{EV}, B_{EV}, and C_{EV}.

In addition, in this case, the encryption key information creation unit 15 creates an element-specific parameter based on a uniform image signal S2 output from the solid imaging element 24 after manufacturing. Therefore, this parameter can be created as information which the manufacturer of the solid imaging element 24 cannot be know. Furthermore, the element-specific parameter is created from a combination of correlation results with the evaluation patterns A_{EV}, B_{EV}, and C_{EV}, not with a variation pattern itself of the solid imaging element 24. Therefore, this parameter can be created as information that the manufacturer of this solid imaging element 24 and a person who stole the solid imaging element 24 cannot know.

Then the encryption key information creation unit 15 creates a plurality of encryption key information D2 ($D2_1$ to $D2_n$) with a prescribed algorithm with thus created element-specific parameter as a seed, and stores or updates the encryption key information D2 in the encryption key information memory 13a of the encryption unit 13.

As a result, the identification information D1 to be given to the encryption unit 13 is converted to encrypted identification information D3 through an encryption process using, for example, encryption key information $D2_1$ unique to this encryption device (solid imaging element 24), and this information is sent to the decryption device 3 via the communication unit 14.

Note that, when the encryption key information creation unit 15 creates a plurality of new encryption key information D2, it can register the plurality of new encryption key information D2 in a database of the decryption device 3 with a prescribed process or by performing a prescribed encryption process on the encryption key information D2 and sending the resultant to the decryption device 3.

As described above, this encryption device 2 encrypts the identification information D1 by using the encryption key information D2 extracted from the element-specific parameter that cannot be known in manufacturing, thus making it possible to significantly improve reliability of an encryption function by strictly avoiding a user pretending a registrant from using the encryption device 2.

(4) Construction of decryption device

The decryption device 3 is composed of a communication unit 30 for communicating information through a communication process under a prescribed radio communication scheme, a requesting unit 31 for making various requests to the encryption devices 2 (2A to 2N), a decoding unit 32 for decrypting encrypted identification information D3 received via the communication unit 30, a comparison unit 33 for performing a prescribed identification process by using a decryption result of the decoding unit 32, and a registration database DB.

This registration database DB stores the formation patterns

of blood vessels of the same parts as the blood vessels to be imaged by the imaging units 11 of the encryption devices 2 (2A to 2N) and a plurality of encryption key information D2 obtained from the same element-specific parameters of the solid imaging elements 24 of the encryption devices 2 (2A to 2N) as registration information D10 ($D10_1$ to $D10_n$).

In this case, the requesting unit 31 requests an encryption device 2 (2A to 2N) being connected via the communication unit 30, for various conditions for an identification process at prescribed timing. The conditions include the number of encryption key information $D2_1$, $D2_2$,..., $D2_n$ to be used out of a plurality of encryption key information, and other matters. In this case, the decryption unit 32 is notified of the number of specified encryption key information.

In addition, the requesting unit 31 makes a request for creating encryption key information D2 if needed. In this case, encryption key information D2 of corresponding registration information $D10_1$, $D10_2$, ..., or $D10_n$ being registered in the registration database DB is updated to encryption key information which is newly created by the encryption device 2 and is obtained through a prescribed registration process or via the communication unit 30.

The decoding_unit 32 reads registration information $D10_1$ corresponding to, for example, the encryption device 2A from the registration database DB based on a transmission source address

written in the header of encryption identification information D3 supplied via the communication unit 30, and selects encryption information $D2_1$ notified from the requesting unit 31 out of the plurality of encryption key information $D2_1$ to $D2_n$ of the registration information $D10_1$.

The decoding unit 32 restores the identification information D1 by performing the same encryption process as the encryption device 2A, on the encrypted identification information D3 by using the encryption key information $D2_1$ being selected, and sends the identification information D1 and corresponding registration information $D10_1$ to the comparison unit 33.

The comparison unit 33 compares the blood vessel formation pattern of the supplied identification information D1 to the blood vessel formation pattern of the corresponding registration information $D10_1$ with a prescribed technique. If the comparison result cannot satisfy a prescribed matching level, the user who is using the encryption device 2A and sent the identification information D1 is determined as a third party and the communication unit 30 is controlled so as to stop communication of information with the encryption device 2A.

When the prescribed matching level is obtained, the comparison unit 34 determines the user using the encryption device 2A sending the identification information D1 as a rightful user. In this case, the comparison unit 33 controls the communication unit 30 so as to communicate information between the encryption

device 2A and an internal information processing unit (not shown).

As described above, the decryption device 3 is capable of performing the identification process by using the identification information D1 (blood vessel formation pattern) unique to a body and the encryption key information D2 obtained from an element-specific parameter unique to the solid imaging element 24.

(6) Operation and Effects of this embodiment

According to the above configuration, this encryption device 2 (2A to 2N) creates an element-specific parameter unique to the solid imaging element 24 based on a uniform image signal S2 output from the solid imaging element 24 as a result of imaging a uniform imaging target by the imaging unit 11.

Then the encryption device 2 (2A to 2N) encrypts the identification information D1 by using the prescribed encryption key information D2 obtained from the element-specific parameter.

Therefore, the encryption device 2 (2A to 2N) is capable of creating encryption key information D2 obtained from the element-specific parameter, which can not be known by third parties even in manufacturing, without previously storing encryption keys in a non-volatile memory, unlike conventional systems, resulting in being capable of ensuring confidentiality of the identification information D1 easily.

According to the above configuration, an element-specific parameter unique to the solid imaging element 24 is created based on a uniform image signal S2 output from the solid imaging element

24 as a result of imaging a uniform imaging target, and the identification information D1 is encrypted with prescribed encryption key information D2 obtained from the element-specific parameter, thus being capable of ensuring confidentiality of the identification information D1 easily and improving reliability of the encryption function.

(6) Other embodiments

Note that the above embodiment has described a case where a creation means for creating a unique parameter of an element group based on a signal output from the element group internally having a plurality of elements as a unit creates an element-specific parameter unique to the solid imaging element 24 based on a uniform image signal S2 output from a plurality of photoelectric conversion elements arranged in the solid imaging element 24. This invention, however, is not limited to this and a unique parameter can be created based on a signal output from, for example, a piezoelectric element group of a touch pad. Alternatively, a unique parameter of an element group having a group of active elements or passive elements as a unit can be created.

In this case, even if the element group is composed of one or plural kinds of elements, the same effects as the above embodiment can be obtained.

Further, the above embodiment has described a case where the creation means creates a unique parameter by directly calculating

hamming distances (correlation values) between data of the uniform image signal S2 output from an element group and three different evaluation patterns A_{EV}, B_{EV}, and C_{EV} being stored in an information memory serving as a storage means and combining the calculation results in a prescribed order. This invention, however, is not limited to this and FFT (Fast Fourier Transform) can be performed on data of the uniform image signal S2 and calculation results of hamming distances of this result and the evaluation patterns A_{EV}, B_{EV}, and C_{EV} can be combined. Alternatively, an inverse FFT can be performed on only data of low frequency components out of a result of the FFT, and the results of hamming distances of the FFT result and the evaluation patterns A_{EV}, B_{EV}, and C_{EV} can be combined. Or these processing results can be combined. By doing this, a unique parameter with high confidentiality and repeatability can be created, thus making is possible to significantly improve reliability of the encryption function.

In this case, the encryption key information creation unit 15 makes the imaging unit 11 image the diffusion plate 25 and creates a unique parameter as encryption key information based on a signal obtained as the imaging result. This invention, however, is not limited to this and the imaging unit 11 can image another uniform imaging target other than the diffusion plate 25, or only a unique parameter can be created without creating the encryption key information. In short, another kind of creation unit for creating a unique parameter can be used.

In addition, in this case, encryption key information is created every time when a request for creating encryption key information is received from the decryption device 3 via the communication unit 14. This invention, however, is not limited to this and other creation timing can be used, such as only manufacturing time.

Further, as an evaluation pattern, a prescribed evaluation pattern is stored in an information memory. This invention, however, is not limited to this and a plurality of evaluation patterns are stored in the information memory and a prescribed number of evaluation patterns can be selected from these evaluation patterns. Alternatively, a different evaluation pattern is selected according to a request of the decryption device 3. Alternatively, an evaluation pattern created with a prescribed algorithm at prescribed timing can be stored in the information memory. By doing this, even if identification information D1 is stolen or even if an evaluation pattern is decrypted from encryption key information, corresponding evaluation pattern cannot be used, thus making it possible to significantly improve reliability of the encryption function.

Furthermore, three kinds of evaluation patterns are stored in the information memory as the number of evaluation patterns. This invention, however, is not limited to this and the same effects as the above embodiment can be obtained, provided that at least two evaluation patterns are stored in the information memory.

Furthermore, the above embodiment has described a case where the encryption unit 13 for encrypting identification information D1 comprising a blood vessel formation pattern by using encryption key information extracted from a unique parameter is applied as an encryption means for encrypting information by using a unique parameter. This invention, however, is not limited to this and an encryption unit for encrypting the identification information D1 by using a unique parameter can be applied.

In this case, a blood vessel formation pattern in a body is encrypted as identification information D1. This invention, however, is not limited to this and another kind of body information such as characteristic pattern existing on a body surface, such as fingerprints, can be encrypted as identification information. In addition, not identification information nor body information but information which is a confidential target can be encrypted.

Industrial Usability

This invention can be used for terminal devices such as personal computers and portable telephones, and household electronic devices in a case of making external devices identify the devices themselves.